5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/697,354	10/29/2003	Brian Harold Kelley	030621	7523

23696 7590 01/08/2007
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	01/08/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 01/08/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
t_ssadik@qualcomm.com

Office Action Summary	Application No.	Applicant(s)	
	10/697,354	KELLEY ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 October 2003 and 07 June 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/15/2006 has been entered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Ellison et al., (U.S. Patent No. 6, 795,905 and Ellison hereinafter).

Regarding claim 1, Ellison discloses a method for selectively enabling operating modes of a device during a device initialization (col. 11, lines 25-45), wherein the operating modes comprise a privileged mode (i.e., isolated execution mode) and a non-privileged mode (i.e., normal execution mode)(col. 4, lines 13-25), and the method comprising:

determining during the device initialization whether the device is to operate in the privileged mode or in both the privileged and non-privileged modes, enabling the privileged mode if it is determined that the device is to operate only in the privileged mode (col. 3, lines 45-67 and col. 4, lines 1-10), and enabling both the privileged (i.e., isolated) and the non-privileged (i.e., normal) modes if it is determined that the device is to operate in both the privileged and the non-privileged modes (col. 2, lines 47-50 and col. 3, lines 6-9)(i.e., Access to an accessible physical memory 60 is governed according to their ring hierarchy and the execution mode. ... the isolated area is accessible only to elements of the operating system and processor operating in an isolated execution mode. The non-isolated area 80 is accessible to all elements of the ring 0 operating system and to the processor), wherein programs operating in the privileged mode have unlimited access to device memory and/or device functions (i.e., the isolated execution ring-0 15, including the operating system nub 16 and the processor nub 18, can access both of the isolated area 70, including applet pages 72

and the nub pages 74, and the non-isolated area 80, including the application pages 82 and the operating system pages 84) and programs operating in the non-privileged mode have limited access to device memory and/or device functions (i.e., the normal execution ring-0 11, including the primary operating system 12 and software drivers 13, and hardware drivers 14, can access both of the non-isolated area 80, including the application pages 82 and the operating system pages 84, but cannot access the isolated area 70)(col. 4, lines 10-45 and col. 12, lines 5-41).

Regarding claim 6, Ellison discloses an apparatus for selectively enabling operating modes of a device during a device initialization (col. 11, lines 25-45), operating modes comprise a privileged mode (i.e., isolated execution mode) and a non-privileged mode (i.e., normal execution mode)(col. 4, lines 13-25), and the apparatus comprising:

a flag (i.e., execution code word), and selection logic that operates to read the flag to set the operating mode of the device, wherein if the flag is set the selection logic enables the privileged mode, and if the flag is not set, the selection logic enables both the privileged and non-privileged modes (col. 2, lines 47-50 and col. 3, lines 6-9)(i.e., the execution mode word is asserted when the processor is configured in the isolated execution mode)(col. 9, lines 30-55 and col. 11, lines 25-45), wherein programs operating in the privileged mode have unlimited access to device memory and/or device functions (i.e., the isolated execution ring-0 15, including the operating system nub 16 and the processor nub 18, can access both of the isolated area 70, including applet

pages 72 and the nub pages 74, and the non-isolated area 80, including the application pages 82 and the operating system pages 84) and programs operating in the non-privileged mode have limited access to device memory and/or device functions (i.e., the normal execution ring-0 11, including the primary operating system 12 and software drivers 13, and hardware drivers 14, can access both of the non-isolated area 80, including the application pages 82 and the operating system pages 84, but cannot access the isolated area 70)(col. 4, lines 10-45 and col. 12, lines 5-41).

Regarding claim 10, Ellison discloses an apparatus for selectively enabling operating modes of a device during a device initialization (col. 11, lines 25-45), operating modes comprise a privileged mode (i.e., isolated execution mode) and a non-privileged mode (i.e., normal execution mode)(col. 4, lines 13-25), and the apparatus comprising:

means for determining during the device initialization whether the device is to operate in the privileged mode or in both the privileged and non-privileged modes , means for enabling only the privileged mode if it is determined that the device is to operate only in the privileged mode (col. 3, lines 45-67 and col. 4, lines 1-10), and

means for enabling both the privileged (i.e., isolated) and the non-privileged (i.e., normal) modes if it is determined that the device is to operate in both the privileged and the non-privileged modes (col. 2, lines 47-50 and col. 3, lines 6-9)(i.e., Access to an accessible physical memory 60 is governed according to their ring hierarchy and the execution mode. ... the isolated area is accessible only to elements of the operating

system and processor operating in an isolated execution mode. The non-isolated area 80 is accessible to all elements of the ring 0 operating system and to the processor), wherein programs operating in the privileged mode have unlimited access to device memory and/or device functions (i.e., the isolated execution ring-0 15, including the operating system nub 16 and the processor nub 18, can access both of the isolated area 70, including applet pages 72 and the nub pages 74, and the non-isolated area 80, including the application pages 82 and the operating system pages 84) and programs operating in the non-privileged mode have limited access to device memory and/or device functions (i.e., the normal execution ring-0 11, including the primary operating system 12 and software drivers 13, and hardware drivers 14, can access both of the non-isolated area 80, including the application pages 82 and the operating system pages 84, but cannot access the isolated area 70)(col. 4, lines 10-45 and col. 12, lines 5-41).

Regarding claim 15, Ellison discloses a computer-readable media comprising instructions, which when executed by a processor in a device, operate to selectively enable operating modes of a device during a device initialization, wherein the operating modes comprise a privileged mode and a non-privileged mode, and the computer-readable media comprising:

instructions for determining during the device initialization whether the device is to operate in the privileged mode or in both the privileged and non-privileged modes (col. 3, lines 45-67 and col. 4, lines 1-10), and

instructions for enabling only the privileged mode if it is determined that the device is to operate only in the privileged mode (figure 2, step 207, column 5, lines 1-2); and

instructions for enabling both the privileged (i.e., isolated) and the non-privileged (i.e., normal) modes if it is determined that the device is to operate in both the privileged and the non-privileged modes (col. 2, lines 47-50 and col. 3, lines 6-9)(i.e., Access to an accessible physical memory 60 is governed according to their ring hierarchy and the execution mode. ... the isolated area is accessible only to elements of the operating system and processor operating in an isolated execution mode. The non-isolated area 80 is accessible to all elements of the ring 0 operating system and to the processor), wherein programs operating in the privileged mode have unlimited access to device memory and/or device functions (i.e., the isolated execution ring-0 15, including the operating system nub 16 and the processor nub 18, can access both of the isolated area 70, including applet pages 72 and the nub pages 74, and the non-isolated area 80, including the application pages 82 and the operating system pages 84) and programs operating in the non-privileged mode have limited access to device memory and/or device functions (i.e., the normal execution ring-0 11, including the primary operating system 12 and software drivers 13, and hardware drivers 14, can access both of the non-isolated area 80, including the application pages 82 and the operating system pages 84, but cannot access the isolated area 70)(col. 4, lines 10-45 and col. 12, lines 5-41).

As per claim 20, Ellison discloses a method for selectively enabling operating modes of a device, comprising:

determining during the device initialization whether the device is to operate in at least one of a privileged mode and a combined privileged and non-privileged mode (col. 3, lines 45-67 and col. 4, lines 1-10), and

enabling the combined privileged and non-privilege mode for each determination that the device is to operate in the combined privileged and non-privileged mode (col. 2, lines 47-50 and col. 3, lines 6-9)(i.e., Access to an accessible physical memory 60 is governed according to their ring hierarchy and the execution mode. ... the isolated area is accessible only to elements of the operating system and processor operating in an isolated execution mode. The non-isolated area 80 is accessible to all elements of the ring 0 operating system and to the processor), wherein programs operating in the privileged mode have unlimited access to device memory and/or device functions (i.e., the isolated execution ring-0 15, including the operating system nub 16 and the processor nub 18, can access both of the isolated area 70, including applet pages 72 and the nub pages 74, and the non-isolated area 80, including the application pages 82 and the operating system pages 84) and programs operating in the non-privileged mode have limited access to device memory and/or device functions (i.e., the normal execution ring-0 11, including the primary operating system 12 and software drivers 13, and hardware drivers 14, can access both of the non-isolated area 80, including the application pages 82 and the operating system pages 84, but cannot access the isolated area 70)(col. 4, lines 10-45 and col. 12, lines 5-41).

Regarding claim 24, Ellison discloses an apparatus, comprising:

a selectable one of a plurality of operating modes, the plurality of operating modes comprising at least a privileged operating mode and a combined privileged and non-privileged operating mode (col. 2, lines 47-50 and col. 3, lines 6-9), a memory comprising a flag (i.e., execution code word) having at least two settings, wherein one predetermined setting of the at least two settings corresponds to the combined privileged and non-privileged operating mode, and selection logic communicatively coupled with the memory and operable to read the flag to set an operating mode of the apparatus, wherein the selection logic is operable to enable the combined privileged and non-privileged mode on the apparatus based on reading the one predetermined setting of the at least two settings (col. 9, lines 15-54), wherein programs operating in the privileged mode have unlimited access to device memory and/or device functions (i.e., the isolated execution ring-0 15, including the operating system nub 16 and the processor nub 18, can access both of the isolated area 70, including applet pages 72 and the nub pages 74, and the non-isolated area 80, including the application pages 82 and the operating system pages 84) and programs operating in the non-privileged mode have limited access to device memory and/or device functions (i.e., the normal execution ring-0 11, including the primary operating system 12 and software drivers 13, and hardware drivers 14, can access both of the non-isolated area 80, including the application pages 82 and the operating system pages 84, but cannot access the isolated area 70)(col. 4, lines 10-45 and col. 12, lines 5-41).

As per claim 2, the method of Ellison discloses the method of claim 1, wherein the step of determining comprises testing a flag (i.e., execution code word)(col. 9, lines 32-54).

As per claim 3, the method of Ellison discloses the method of claim 1, wherein the step of enabling only the privileged mode comprises controlling one or more device memory management units to enable only the privileged mode (i.e., the isolated execution mode)(col. 9, lines 15-54, where it is inherent that the processor contains a MMU to manage communications with memory).

As per claim 4, the method of Ellison discloses the method of claim 1, wherein the step of enabling both the privileged mode and the non-privileged modes comprises controlling one or more device memory management units to enable both modes (col. 2, lines 64-67 and col. 3, lines 1-67, and col. 4, lines 1-10, where it is inherent that the processor contains a MMU to manage communications with memory).

As per claim 5, the method of Ellison discloses the method of claim 1, wherein the device is a wireless device (col. 2, lines 47-67 and col. 3, lines 1-67, and col. 4, lines 1-10, where the logical operating architecture may be realized to be deployed on a laptop).

As per claim 7, the apparatus of Ellison discloses the apparatus of claim 6, further comprising a memory that stores the flag (i.e., execution code word)(col. 9, lines 32-54).

As per claim 8, the apparatus of Ellison discloses the apparatus of claim 6, further comprising one or more memory management units that are controlled by the selection logic (i.e., comparator 314) to set the operating mode of the device (col. 10, lines 1-50, where it is inherent that the processor contains a MMU to manage communications with memory).

As per claim 9, the method of Ellison discloses the method of claim 6, wherein the device is a wireless device (col. 2, lines 47-67 and col. 3, lines 1-67, and col. 4, lines 1-10, where the logical operating architecture may be realized to be deployed on a laptop).

As per claim 11, the apparatus of Ellison discloses the apparatus of claim 10, wherein the means for determining comprises means for testing a flag (i.e., execution code word)(col. 9, lines 15-54 and col. 10, lines 1-50).

Regarding claim 12, the apparatus of Ellison discloses the apparatus of claim 10, wherein the means for enabling the only privileged mode comprises means for controlling one or more device memory management units to enable only the privileged

mode (col. 2, lines 64-67 and col. 3, lines 1-67, and col. 4, lines 1-10, where it is inherent that the processor contains a MMU to manage communications with memory).

As per claim 13, the apparatus of Ellison discloses the apparatus of claim 10, wherein the means for enabling both the privileged mode and the non-privileged modes comprises means for controlling one or more device memory management units to enable both modes (col. 2, lines 64-67 and col. 3, lines 1-67, and col. 4, lines 1-10, where it is inherent that the processor contains a MMU to manage communications with memory).

As per claim 14, the method of Ellison discloses the method of claim 10, wherein the device is a wireless device (col. 2, lines 47-67 and col. 3, lines 1-67, and col. 4, lines 1-10, where the logical operating architecture may be realized to be deployed on a laptop).

As per claim 16, the computer-readable media of Ellison discloses the computer-readable media of claim 15, wherein the instructions for determining comprise instructions for testing a flag (i.e., execution code word)(col. 9, lines 15-54 and col. 10, lines 1-50).

As per claim 17, the computer-readable media of Ellison discloses the computer-readable media of claim 15, wherein the instructions for enabling the only privileged

mode comprise instructions for controlling one or more device memory management units to enable only the privileged mode (col. 2, lines 64-67 and col. 3, lines 1-67, and col. 4, lines 1-10, where it is inherent that the processor contains a MMU to manage communications with memory).

As per claim 18, the computer–readable media of Ellison discloses the computer-readable media of claim 15, wherein the instructions for enabling both the privileged mode and the non-privileged modes comprise instructions for controlling one or more device memory management units to enable both modes (col. 2, lines 64-67 and col. 3, lines 1-67, and col. 4, lines 1-10, where it is inherent that the processor contains a MMU to manage communications with memory).

As per claim 19, the method of Ellison discloses the method of claim 15, wherein the device is a wireless device (col. 2, lines 47-67 and col. 3, lines 1-67, and col. 4, lines 1-10, where the logical operating architecture may be realized to be deployed on a laptop).

As per claim 21, the method of Ellison discloses the method of claim 20, wherein determining further comprising reading a flag in a memory of a device, the flag having at least two settings, wherein one predetermined setting of the at least two settings corresponds to the combined privileged and non-privileged operating mode (col. 2, lines 64-67 and col. 3, lines 1-67, and col. 4, lines 1-10 and col. 9, lines 13-67, where

configuration storage 250 stores the data that is used to assert the execution mode word 253).

Regarding claim 22, the method of Ellison discloses the method of claim 20, wherein enabling further comprises:

partitioning (i.e. isolating) a code memory portion of the memory of the device into a privileged code region comprising privileged code (i.e., isolated area 70, Fig. 1B, element 74) and a non-privileged code region comprising non-privileged code (i.e., non-isolated area 80, Fig. 1B, element 84), and partitioning (i.e., isolating) a data memory portion of the memory of the device into a privileged data region comprising privileged data (i.e., isolated area 70, Fig. 1B, element 72) and a non-privileged data region comprising non-privileged data (i.e., non-isolated area 80, Fig. 1B, element 82)(col. 4, lines 10-45).

Regarding claim 23, the method of Ellison discloses the method of claim 22, wherein enabling further comprises restricting operation of the non-privileged code (i.e., applications 1-N, Fig. 1B, element 41, and Ring-0, Fig. 1B, element 11) to the non-privileged code region of the code memory (i.e., non-isolated area 80, Fig. 1B, element 84) and to the non-privileged data region of the data memory (i.e., non-isolated area 80, Fig. 1B, element 82)(col. 4, lines 10-45).

Regarding claim 25, the apparatus of Ellison discloses the apparatus of claim 24, wherein the memory further comprises a code memory and a data memory, further comprising:

wherein the code memory is operable to store code (i.e., NUB pages 74 and OS pages 84)(col. 4, lines 10-50), a first memory management unit operable, under control of the selection logic, to partition (i.e., isolate) the code memory into a privileged code region comprising privileged code and a non-privileged code region comprising non-privileged code (col. 8, lines 20-67 and col. 9, lines 1-67), wherein the data memory is operable to store data (i.e., Applet pages 72 and Application pages 82)(col. 4, lines 10-50), and a second memory management unit operable, under control of the selection logic, to partition the data memory into a privileged data region comprising privileged data and a non-privileged data region comprising non-privileged data (col. 8, lines 20-67 and col. 9, lines 1-67).

Regarding claim 26, the apparatus of Ellison discloses the apparatus of claim 25, wherein the first memory management unit is operable to restrict operation of the non-privileged code to the non-privileged code region of the code memory, and wherein the second memory management unit is operable to restrict operation of the non-privileged code to the non-privileged data region of the data memory (i.e., Access to an accessible physical memory 60 is governed according to their ring hierarchy and the execution mode. ... the isolated area is accessible only to elements of the operating system and processor operating in an isolated execution mode. The non-isolated area 80 is

accessible to all elements of the ring 0 operating system and to the processor)(col. 4, lines 10-45).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

McGrath et al., (U.S. Patent Publication 2004/0210764).

England et al., (U.S. Patent No. 6,651,171),

Freeman et al., (U.S. Patent No. 6,925,570), and

Diamant et al., (U.S. Patent No. 6,268,789).

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.
Patent Examiner
Group 2131
Dec. 26, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER